DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MEDICAL DEPARTMENT CENTER AND SCHOOL
AND FORT SAM HOUSTON
2250 STANLEY ROAD
FORT SAM HOUSTON, TEXAS 78234-6100

REPLY TO
ATTENTION OF
MCCS-BIM

26 NOV 2002

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Installation Information Management Policy 25-02, Compromised Computer Systems

1. REFERENCE. Unclassified message, HQDA, SAIS-IOA, 172032Z Oct 01, subject: Compromised Computer Systems Policy.

2. PURPOSE. This policy clarifies actions required by users, as well as system and network administrators in response to a system compromised by a worm, malicious code, or unauthorized access gained by an intruder.

3. SCOPE. This memorandum applies to all organizations located on Fort Sam Houston, Camp Bullis, and Camp Stanley, that have connectivity to the installation network managed by the Information Technology Business Center, and includes both Government-owned and leased automation equipment.

4. BACKGROUND. This policy was formulated to improve security and reliability of the Fort Sam Houston computing environment and to ensure compliance with the referenced message.

5. POLICY. If a system administrator or user suspects that a computer may be compromised by a worm, malicious logic, or unauthorized access has been gained by an intruder, they will take the following actions:

a. Do not turn the system off.

b. Immediately contact the ITBC Help Desk and stop anyone else from accessing the system.

c. Immediately isolate the system from the network and prevent all access to the system. Isolation includes physical isolation (unplugging the network connection and restricting any direct physical access to the wall jack, while leaving the power on), which may be accomplished by the user, and logical isolation (blocking the IP at security routers or firewalls both inbound and outbound) from the network, which will be accomplished by ITBC technical staff.

d. The ITBC will immediately notify the supporting Regional Computer Emergency Response Team (RCERT), and make appropriate notifications to the Fort Sam Houston Information Assurance Officer and chain of command. Failure to notify the RCERT is a violation of Army regulations cited in the reference and could result in criminal or administrative disciplinary actions.

e. Army Computer Emergency Response Team (ACERT) or RCERT will provide guidance to the ITBC staff to obtain the forensic physical evidence required to support an investigation. The ITBC will be prepared to provide the hard drive from the system, but will not remove it until the lead investigative agency provides the guidance and requirements.

f. Once a drive has been returned to ITBC, the drive will be reformatted using a low-level format method and have the Operating System reinstalled and patched. The ITBC will request a vulnerability assessment from the ACERT or RCERT prior to bringing the system back online. The Internet Protocol for the compromised system will be unblocked temporarily only to scan and will only be removed permanently after the system has had all identified vulnerabilities fixed and rescanned.

6. Systems verified as compromised with a known worm or through scripts that have automated scanning and installation processes, such as, but not limited to Code Red or the SADMIN/IIS worm, are considered compromised systems and will be reported to your RCERT, your Fort Sam Houston Information Assurance Officer and chain of command. Neither ITBC nor users will utilize freeware removal tools unless the tool has been verified by ACERT as meeting the requirements necessary to adequately remove all components of the worm. The ITBC will rebuild and patch systems compromised, even if an automated script that could install a backdoor, or Trojan Horse within the OS or applications, is <u>not</u> readily visible. This is the only acceptable security solution for these compromised systems. A vulnerability assessment will be conducted on the rebuilt system.

7. This policy will be reviewed 1 year from the implementation date.

8. The point of contact is Mr. Mike Merrill, Information Technology Business Center, 221-5281, or email address Michael.Merrill@us.army.mil.

DARREL R. PORR
MG, US Army
Commanding

DISTRIBUTION:
A